Facebook Data Breach

Zakiria A Jordan

Professor Gladden

CYSE 300

November 30, 2024

The Facebook Data Breach of 2019 was a very popular cybersecurity attack. There were weaknesses in Facebook's security infrastructure compromising the personal information of millions of users. The most serious of these was related to a set of poorly secured third-party apps with access to user data through Facebook's platform. These apps had too broad permissions and were able to collect an enormous amount of information from both users and their friends. Another vulnerability was in Facebook's password recovery process, which allowed attackers to reach unencrypted user passwords stored as plain text in Facebook's internal systems and make access easier. Moreover, the poor authentication practices of the platform and the lack of tougher controls on sharing user data with third-party developers left it prone to breaches.

The vulnerability of the situation was exploited by malicious players who seized on these vulnerabilities, thereby granting unauthorized access into Facebook systems. The perpetrators employed certain tactics, scraping included, to collect private information: email addresses, phone numbers, and additional personal data that were supposed to remain protected. Although Facebook initially denied that hackers had accessed the data with unauthorized access, it later emerged that data scraping involved the use of vulnerabilities in the social network's API to access and pull data in massive amounts from public profiles.

The consequences of the breach of data at Facebook were vast. It not only compromised personal information from over 530 million users worldwide but also caused immense damage to its reputation. People's faith in the firm was dented so much that public outcry and increased regulator scrutiny followed in suit. Actions from various government agencies include several fines: a $5 billion fine by the FTC (Federal Trade Commission) from the United States

government for its fault due to the data breach, apart from heightening concern and fostering ongoing debates about data privacy and responsibilities of technology companies to keep user information private.

The consequences could have been minimal, or such incidents could even have been avoided if strong cybersecurity measures were in place on the part of Facebook. It could have bettered security around APIs, allowing external applications to access a certain amount of data while even that access was strictly and clearly defined by user permissions. Other important measures would have been the introduction of end-to-end encryption for sensitive user data stored internally, and the storage of passwords in a secure way by hashing and salting rather than in plain text. Furthermore, Facebook should have introduced more intensive monitoring and auditing of its developer ecosystem to ensure that third-party apps complied with more stringent data protection policies. Finally, Facebook could do more to educate users on security features, encouraging the use of two-factor authentication and other steps to protect accounts from unauthorized access.

Resources

Bowman, E. (2021, April 9). ***After Data Breach Exposes 530 Million, Facebook Says It Will Not Notify Users*****. NPR; NPR.** **https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users**

Twingate Team. (2024, February 22). ***What happened in the Facebook data breach?*** **|** ***Twingate*****. Www.twingate.com. https://www.twingate.com/blog/tips/facebook-data-breach**

Clark, M. (2021, April 6). ***The Facts on News Reports About Facebook Data*****. About Facebook. https://about.fb.com/news/2021/04/facts-on-news-reports-about-facebook-data/**